DOI 编码：10.13646/j.cnki.42-1395/u.2022.09.021

船闸自动化控制系统信息安全防护体系研究

刘相莹[1]，陈拥军[2]

（1. 北京六方云信息技术有限公司，北京 100000；2. 南京苏润科技发展有限公司，江苏 南京 210000）

摘　要：随着信息化与自动化的两化融合发展，工控系统信息安全面临着巨大的安全挑战，层出不穷的工控安全事件推动了工控系统信息安全防护体系的建设和研究。本文阐述了作为工控系统一个分支的船闸自动化控制系统的现阶段面临的安全问题及挑战，结合当前的信息安全防护技术和六方云项目实践，从技术的角度提出了现阶段可行的信息安全防护体系，并分析其未来的发展方向。

关键词：船闸；信息安全；传输加密；本体保护

中图分类号：U641　　**文献标识码：**A　　**文章编号：**1006—7973（2022）09-0061-03

1 前言

船闸作为重要的水上交通枢纽，随着水运经济的发展，日益增加的过闸需求和实际能力推动了船闸自动化控制系统的发展。借助于先进的控制技术、通信技术、传感器技术以及监控技术，逐步由船闸自动化向自动化船闸、智慧船闸发展，极大促进了航区和流域水运经济的发展[1]。

船闸自动化控制系统在带来效率提升和智能化的同时，由于数据开发带来网络架构的变化、访问和控制的双向数据交换等需求，相对于传统的运行模式，必然会增加系统的设备安全和数据安全隐患。为了避免例如黑客入侵、勒索、蠕虫等病毒的干扰，需要保障船闸的自动化控制系统和信息系统的安全符合国家相关规定。避免作为关键信息基础设施的船闸枢纽作为达成其目的的攻击目标，导致系统宕机无法运行。近年来，诸如伊朗“震网”病毒事件等工控系统信息安全事件频繁发生，造成工业设施运行异常，甚至造成工业配方资料失窃、停工停产等严重事故，因此船闸自动化控制系统信息安全防护体系建设势在必行。

2 船闸自动化控制系统概述

2.1 船闸的主体构成

船闸在物理建筑上分为上闸首工作闸门、上闸首输水阀门、闸室、下闸首工作闸门、下闸首输水阀门等，其主体的平面图如图 1 所示：

图 1 船闸的平面结构图

2.2 船闸运行的控制方式

船闸高效、安全、可靠运行，离不开船闸的运行控制。目前，船闸运行控制分为集中控制和分散控制两种，集中控制是在监控中心实现的程序运行，分散控制是指运行人员在上下游闸首操作台上分别实现闸阀门的程序运行，单向运行及闸阀门的单侧点动运行。这两种控制方式都是由船闸自动化控制系统完成的。脱离船闸自动化控制系统的手动应急操作（如急停）是在测试和紧急情况下使用[2]。正常过闸流程如图 2。

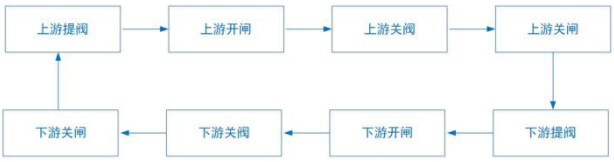

图 2 正常过闸流程图

2.3 船闸自动化控制系统组成

船闸自动化控制系统是工业集中分散控制系统，操作和信息终端较多，集控中心监控三级构成。其网络结构可分为三层：

现场设备层：主要包括：电机拖动控制柜、操作台、液压泵站、以及外围传感器（水位计、闸 / 阀门开度仪、限位开关），以及其他辅助设备如交通灯、广播和照明系统等。

现地控制层：主要包括：可编程控制器核心器件、计算机设备、工业交换机等。现地控制层功能实现船闸就近控制，及时处理船闸运行工况，同时还具备紧急突发情况下的应急保障功能，还具备停航期间船闸的养护和维修功能。以确保船闸运行安全畅通。

集中监控层：包括由数据库服务器、船闸中心工程师站、操作员站、集控操作台、大屏幕显示系统、网络设备及打印机等组成。主要实现船闸正常运行的“少人值守、高效过闸”的功能。同时具备对船闸运行工况、设备状态管理、巡察巡检等数据统计分析并上传至上一级管理单位。并对上一级管理单位发出的数据采集需求和远程控制需求给予准确及时响应。

3 船闸自动化控制系统信息安全风险

（1）系统网络边界缺乏控制隔离机制。船闸与枢纽管理处之间缺乏有效的隔离措施，，一旦有网络攻击，不能有效的阻断和隔离，将难以遏制网络攻击扩散造成严重的影响。

（2）数据传输缺少加密认证措施。船闸的数据通过专线传输到枢纽管理处，在这个过程中存在网络传输数据被窃听和篡改的风险，应采用安全可靠的加密算法对数据传输过程进行密码化处理。

（3）控制系统严重漏洞难以及时处理。由于目前市面上可编程控制器多是进口品牌，存在安全隐患，容易被黑客利用，形成远程攻击，同时面临硬件版本和编程软件难以在线升级、相关漏洞发布周期长等问题，难以及时处理威胁严重的漏洞。

（4）病毒与入侵行为防护能力不足。为了保证控制系统的可用性，操作员站、数据服务器等计算机终端设备未进行安全防护，对 U 盘等输入存储设备未进行管理。病毒库长期得不到更新，而且杀毒软件对新病毒的处理总是滞后的，有时也会造成软件误杀。

（5）缺乏安全意识和数据安全等行为审计能力。相关操作人员未经过相关安全教育和培训，导致发生错误操作，给自动化控制系统留下安全隐患。同时自动化控制系统在相对封闭网络架构下，空余网络端口、未经许可的输入设备等接入给管理带来非常大的困扰。另外，对系统中的数据存储和转发做不到可追溯，也是系统的主要安全风险之一。

（6）非常时期运行维护的安全风险。控制系统的网络设备在硬件和软件的安全性防护水平不一，需要第三方定期维护控制系统采用的控制器和设备的种类繁多，外来厂商人员的定期运行维护成为一个潜在的安全风险点。虽然从管理上保障运维过程的可管理，但是在没有有效技术手段支撑的情况，本地管理人员很难监测到外部人员的越权操作或者故意改变运行逻辑的行为，在出现问题时，也很难追踪定位。

（7）移动介质缺乏有效管控。日常运维工作中存在使用移动介质拷贝数据及文件的操作。文件拷贝的介质无法做到专盘专用。从已经发生的安全事件看，移动介质是一个重要的传播恶意代码到控制系统环境的路径[3]。

（8）控制系统安全制度不完善，缺乏安全意识。船闸针对业务系统制定了完善的管理制度、管理流程，但未制订自动化控制系统的网络安全和数据安全的相关操作流程、权限和制度，未形成有针对性的的安全管理制度体系。未对相关工作人员定期培训和持证上岗，导致人员安全意识薄弱成为导致安全风险的重要因素。

4 船闸自动化控制系统信息安全防护体系

船闸自动化控制系统信息安全防护设计在遵循船闸业务特点的前提下，力求满足工控系统等保 2.0 的安全要求，结合六方云在船闸自动化控制系统信息安全防护项目实践，从“边界防护、传输加密、本体保护、入侵检测、行为审计、安全管控”等 6 个方面进行落地，从而实现“异常行为可监测、安全威胁可防御、安全价值可呈现”。

4.1 边界防护

在船闸监控调度中心数据出口部署工业防火墙，采用逻辑隔离措施，实现逻辑隔离、报文过滤、访问控制等功能，阻止网络攻击跨边界扩散渗透，有效保护自动化控制系统的安全。同时基于工业协议及操作行为白名单防护技术，建立工业协议及操作行为安全基线，阻止一切不可信的数据和操作行为，最大程度的防范已知与未知威胁。

4.2 传输加密

在枢纽管理处端同步部署工业防火墙，基于六方云工业防火墙 IPSec 协议的 VPN 技术，支持 ESP 和 AH 协议，加密算法支持 3DES、DES、AES，验证算法支持 MD5、SHA1、SHA256[4]，建立船闸到枢纽管理处之间的虚拟加密通道，有效保护船闸数据传输过程中的完整性及保密性需要，防止第三方设备非法入侵。

4.3 本体保护

（1）控制系统软件保护。控制系统对可用性、实时性要求较高，需部署通过国家有关机构的安全检测认证的终端白名单防护软件，基于应用程序、网络和操作行为白名单技术，防范恶意软件或恶意代码的植入，同时使工作站主机免受病毒等各种非法攻击，可以有效管控主机的 USB 等外部端口。

（2）控制单元（PLC）保护。控制单元（PLC）作为船闸自动化控制系统最核心的设备，需要重点保护。结合控制单元（PLC）部署环境相对恶劣的特点，部署具有六方云网络防护设备新型外观专利的工业防火墙[5]，具有工业级芯片和电子元器件、无风扇、支持工业宽温的一体化设计，基于工业协议如 ModbusTCP/IP、Profinet 等的识别和深度解析，进行指令级的细粒度管控。

（3）入侵检测。在汇聚交换机旁路部署入侵检测系统，采用六方云通信数据检测方法专利技术[6]，合理设置检测规则，及时捕获网络异常行为、分析潜在威胁，及时发现、报告并处理包括病毒木马、端口扫描、暴力破解、异常流量、协议包伪造等网络攻击或异常行为。

4.4 行为审计

在汇聚交换机旁路部署控制网络审计系统，基于对

工业协议深度解析与操作行为的安全审计，实时检测控制系统中的未经许可的 IP 端口、未经许可的设备、未经许可人员的操作以及异常数据传输进行记录并实时报警，包括对系统一定时期内符合标准工业协议的通信行为提供历史记录，保证可追溯性，为船闸自动化控制系统的安全调查提供依据。

4.5 安全管控

构建安全管理中心，对部署的安全技术设备进行集中管控，将分散的、孤立的安全设施整合成一个有机的整体，能够协同工作，更好的发现问题、解决问题，从而实现安全管理的可持续运营，提高安全防护体系的运维效率。

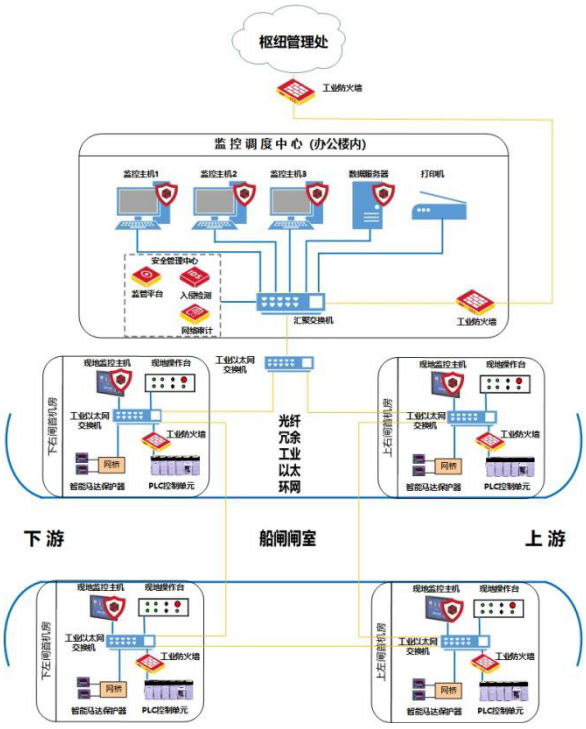

图 3 船闸自动化控制系统安全防护体系示意图

5 船闸自动化控制系统信息安全防护发展方向

随着传统水运日趋数字化、网联化，并且有物联网、大数据、人工智能技术等新技术加持，未来船闸将更智慧。船闸自动化控制系统必将应用工业互联网等先进技术，推动数字化转型，促使自动化控制系统与调度系统、安防系统、广播系统、地理信息系统（GIS）、航道监管系统的深度融合，真正使船闸做到信息集中、资源共享、统一管理，航道管理更智能、更高效。系统的互连互通，数据共享，其面临的安全风险将更复杂多样。基于这样的现状，未来船闸自动化控制系统信息安全防护可从以下几个方面持续推进：

（1）应用态势感知、AI 人工智能高级威胁检测等新技术，构建主动防御体系。随着船闸控制系统信息安全防护体系的建立，以应用环境的安全大数据为基础，以控制与管理系统可用性、安全性监控为主线，通过将多种安全数据、信息和情报进行统一收集，由专业人员进行分析、解释、显示和处置，主动、及时地发现安全问题，并调度资源解决问题，形成船闸的主动式信息安全防护新局面。

（2）提升控制系统数据安全保护能力，防范数据攻击；采取数据融合等相关技术，提升数据融合处理和智能处理能力。

（3）强化安全运维管理，加强对环境、资产、介质、设备维护、配置等方面的管理，制定应急预案并定期开展应急演练，提高安全防护意识和应急处理能力。

（4）加强控制网络安全教育培训和人才培养，建立既具备信息安全技术能力，能够正确的使用、配置、维护常规的安全设备，又具有自动化控制系统理论知识、实操能力、运维能力的复合型人才队伍。

6 结语

本文通过对船闸自动化控制系统的组成及现状分析，指出其现阶段面临的信息安全风险，并根据这些风险和政策合规性要求，研究并提出了可行的信息安全防护思路，介绍了现阶段的安全防护措施及技术，从技术角度构建一套行之有效的信息安全防护体系，在实现 OT 与 IT 两网融合的同时，确保系统网络和数据的安全性。当然，由于船闸自动化控制系统需面向未来智慧船闸的发展需要，很多信息安全防护手段还处在探索阶段，还有待在以后的工作实践中不断总结和研究。

参考文献：

[1] 赵阳，王国伟. 智能化集中控制在智慧船闸建设中的应用探索［J］. 中国水运，2016，16（2）：124 — 126.

[2] 鲍晓兵. 船闸自动控制系统［J］. 机械工程与自动化，2014，185（4）：162 — 163.

[3] 王智民. 工业互联网安全［M］. 北京：清华大学出版社，2020.

[4] 汪付强，杨明，王智民，王鑫，张建强，张鹏，刘祥志. 工业互联网安全传输装置［P］. CN：ZL 2021 2 2959907.9，2021-12-24.

[5] 王智民，赵学全，文武. 网络防护设备［P］. CN：ZL 2019 3 0296083.7，2020-1-27.

[6] 王高杰，李思齐，王智民，何志福. 网络的通信数据检测方法、装置以及机器可读存储介质［P］. CN：ZL 2018 1 1399478.0，2020-12-18.